The primary necessity for any PAKE protocol is, two entities (users/devices etc.) want to establish a session key based on a (short potentially weak) string (like a password).

SoK: Password-Authenticated Key Exchange – Theory, Practice, Standardization and Real-World Lessons

Feng Hao
University of Warwick
United Kingdom
feng.hao@warwick.ac.uk

Paul C. van Oorschot
Carleton University
Canada
paulv@scs.carleton.ca

PAKE is necessary in scenarios when two parties (say two devices) want to communicate with one another and there is no PKI available and there is no scope of using any biometrics. In such cases, using password as means of authentication to derive the new session key is the solution, hence PAKE is necessary.

ABSTRACT

Password-authenticated key exchange (PAKE) is a major area of cryptographic protocol research and practice. Many PAKE proposals have emerged in the 30 years following the original 1992 Encrypted Key Exchange (EKE), some accompanied by new theoretical models to support rigorous analysis. To reduce confusion and encourage practical development, major standards bodies including IEEE, ISO/IEC and the IETF have worked towards standardizing PAKE schemes, with mixed results. Challenges have included contrasts between heuristic protocols and schemes with security proofs, and subtleties in the assumptions of such proofs rendering some schemes unsuitable for practice. Despite initial difficulty identifying suitable use cases, the past decade has seen PAKE adoption in numerous large-scale applications such as Wi-Fi, Apple's iCloud, browser synchronization, e-passports, and the Thread network protocol for Internet of Things devices. Given this backdrop, we consolidate three decades of knowledge on PAKE protocols, integrating theory, practice, standardization and real-world experience. We provide a thorough and systematic review of the field, a summary of the state-of-the-art, a taxonomy to categorize existing protocols, and a comparative analysis of protocol performance using representative schemes from each taxonomy category. We also review real-world applications, summarize lessons learned, and highlight open research problems related to PAKE protocols.

CCS CONCEPTS

• **Security and privacy → Cryptography**.

KEYWORDS

Password authenticated key exchange; PAKE; key exchange

ACM Reference Format:
Feng Hao and Paul C. van Oorschot. 2022. SoK: Password-Authenticated Key Exchange – Theory, Practice, Standardization and Real-World Lessons. In *Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS '22), May 30-June 3, 2022, Nagasaki, Japan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3488932.3523256

ASIA CCS '22, May 30-June 3, 2022, Nagasaki, Japan

ACM ISBN 978-1-4503-9140-5/22/05…$15.00
https://doi.org/10.1145/3488932.3523256

1 INTRODUCTION

While user-chosen passwords remain widely used for authentication [20], many password-based protocols are vulnerable to offline guessing attacks [99]. This motivates use of *password-authenticated key exchange* (PAKE) protocols, dating to Bellovin and Merritt's 1992 *Encrypted Key Exchange* (EKE) [15]. EKE allows two parties to establish a high-entropy session key with authentication based on a low-entropy shared password without being subject to offline guessing attacks. Distinct from earlier work [73], EKE *does not* require a trusted third party or public-key infrastructure (PKI).

Many PAKE proposals and variants followed, some with new theoretical models to support rigorous analysis. The area also attracted strong industrial interest, including prolonged patent disputes in the 2000s [21]. To reduce confusion and encourage deployment, standards bodies including IEEE, ISO/IEC and IETF have pursued the standardization of PAKE protocols—helping move them from academic study to commercial use. These activities suggest a PAKE research timeline with three main periods: 1992–2008, 2008–2018, and 2018–present. (Fig. 1 in Section 2.1 gives further details.)

Thirty years of PAKE research has left a field rich in theory, practice, standardization—and also real-world lessons, many extending to broader areas of cryptography and security. PAKE research has also led to many interesting questions. For example, a typical PAKE protocol involves only 2 or 3 flows of messages; why is a protocol involving so few messages, so difficult to get right? Of the many provable secure PAKE protocols proposed, why are so few used in practice? How did the standardization of PAKE proceed, and how is it that several *standardized* PAKE protocols are still found to have vulnerabilities? If PAKE protocols appear naturally resistant to phishing attacks, why have they not replaced password authentication in web applications?

Answers to these questions appear not yet to have been pursued in broad, organized manner in one place, or are absent. This motivates our comprehensive review and systematization of PAKE protocols. We review the theory, practice, standardization and real-world applications of PAKE, and draw lessons accordingly. Our contributions include the following.

- We systematically review major PAKE proposals from the past 30 years, including recent updates.
- We categorize PAKE protocols by their main properties and design strategies, and offer a taxonomy.
- Using selected PAKE category representatives, we compare performance of state-of-the-art protocols delivered by the leading design approaches.
- We review real-world applications that use PAKE, and discuss the pros and cons of using these protocols versus non-PAKE alternatives.